Invasion of Malware Evading the Behavior-based Analysis

Memory-Based Exploit Analysis of AhnLab MDS

Feb. 21, 2014

AhnLab

Content

Introduction

Multiple security vendors have emphasized and adopted “signature-less” analysis technology to detect unknown malware for their advanced persistent threat (APT) defense solutions. The “signature-less” analysis technology that those vendors insist is behavior analysis based on a virtual machine or sandbox. It is, however, no longer effective to detect unknown malware by depending on sandbox-based behavior analysis. Since cyber criminals create malware that incorporates new mechanisms to bypass an automated sandbox-based analysis system, malware has become more sophisticated and more rampant than ever.

This paper explores the limitations of sandbox-based behavior analysis, and introduces the differentiated approach that AhnLab MDS provides with its exclusive technologies and features.

Ever-evolving Malware Bypass Even Sandbox-based Behavior Analysis

In November 2012, AhnLab Security E-response Center (ASEC) obtained a remarkable malware sample. This sample was distributed via an email attachment with the subject line reading, “Evaluation and Diagnosis of the Status of the Republic of Korea Air Force.” The attached document file contained details about the prospects of the Korea Air Force and public awareness towards South Korean air power. Understandably, most email recipients or users would recognize this file as an important document on national defense. This shows that the attacker launched the attack with an understanding of the target’s predictable behavior patterns.

In terms of technique, this file was sophisticated and elaborately designed. In order to bypass heap-spray detection, a very small amount of heap-spray was generated while the file was being loaded. Also, the malware embedded in this file was set up to run only when the file was opened with the latest version of the software.

When the user opened this file with the latest version of the software, the document on the Korea Air Force was displayed. At that point, no malicious behavior occurred nor was the shellcode executed. Since there was no malicious behavior detected, behavior-based APT defense solutions only discerned that this file was normal instead of “suspicious” or “malicious.”

However, this file was certainly malicious. What was the secret behind this malicious file’s penetration?

A certain user interaction is required to launch malicious behavior in this file: when a curious user opens the file and scrolls down to read the content. When the user reaches the paragraph, “Issues and Concerns” on the second page, a malicious file named “HncCtrl.exe” is automatically created and executed. “HncCtrl.exe” is executed to generate another malicious file which steals private information from the PC and sends it to a specific email address. In other words, the attacker designed the malicious document to begin to exploit when triggered by a specific user interaction. This is a type of the latest APTs, which are able to bypass the automated sandbox-based analysis system.

Limitations of Sandbox Behavior Analysis

Recently, many security vendors have insisted on the importance of “signature-less” analysis technology for identifying unknown malware which cause severe damage, including sensitive data leakage. Some of the vendors assert that behavior-based analysis is the only signature-less method to detect unknown malware. If so, would the sandbox-based behavior analysis be able to detect ever-evolving malware?

Unfortunately, the answer to this question is “Not all of them.” There are limitations to APT defense solutions which detect malware using a sandbox-based behavior analysis.

“Sandbox-based behavior analysis” is a mechanism to discern whether a sample file is malicious or normal by executing the sample file in a “sandbox,” i.e., a restricted and controlled environment. Thus, in order for this mechanism to respond and solve the problem, the malware must execute its behavior in the exact same manner as intended in the sandbox. However, recent attacks have started to use non-executable files such as document files that display or perform no discernible behaviors, and thus bypass the automated sandbox-based analysis system.

Three types of the latest malware that have bypassed the sandbox-based analysis system are discussed below:

1. Interactive malware that waits for specific user interaction to perform malicious behavior

In addition to the document files mentioned above, there has also been a PDF file that did not trigger any malicious behavior until a user scrolls down to a specific page.

In another case, malware in an already infected PC was executed only when there was a specific change in the input device such as by clicking or moving the mouse in a specific direction; a popup window warning was then displayed indicating that the PC was infected. Only when the user clicked the “OK” button of the popup window was the malicious behavior of the malware executed.

Since these types of malware do not activate or display any suspicious or malicious behavior until there is a specific user interaction, it is almost impossible to detect them using APT defense solutions with sandbox-based behavior analysis.

2. Time-consuming malware that are difficult to control in an automated analysis system

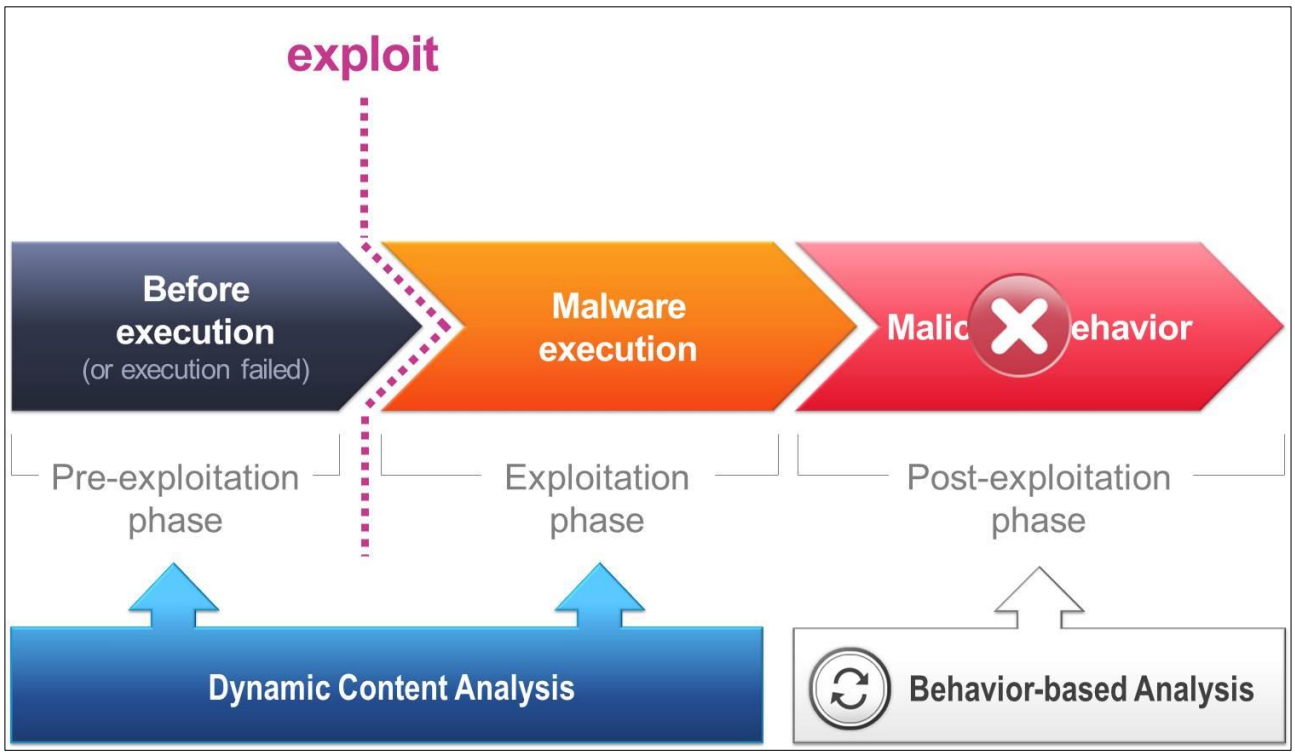
Most APT defense solutions use controlled environments such as a virtual machine or sandbox to analyze behavior automatically. Due to the limitations of hardware resources in analysis systems, however, it is difficult to keep the virtual machine or sandbox in operation until the behavior of malware has fully taken place. Taking advantage of this limitation, attackers create malware with “scheduling” techniques to execute behaviors at a specific time. This is called a “time-bomb” or “Trojan nap.” This time-bomb method requires some specific APIs such as a sleep API, and there are some APT defense solutions that classify a program as malware if it uses one of those specific APIs. However, this can cause false positives since the corresponding APIs are also used in normal programs.

3. Intelligent malware that is aware of the sandbox or virtual machine and hides its malicious behavior

This type of malware is designed to evade not only detection and analysis by APT defense systems but also malware researchers who generally use virtual machines or sandboxes for dynamic analysis. Some APT defense solutions detect an “attempt” to recognize various changes in virtual machines or sandboxes, such as the changes of currently running processes, registry keys and values, and virtual hardware. However, malware can be aware of this “detection” and refrain from executing malicious behavior in these circumstances. Recent malware have been continuously evolving to evade virtual machines or sandboxes analysis with various advanced techniques.

Memory Analysis-based Exploit Detection of AhnLab MDS

AhnLab MDS implements a new analysis technology to detect malware that attempt to bypass behavior analysis. Dynamic Intelligent Content Analysis (DICA) is an exclusive technology that analyzes malware based on assembly codes in the memory. With this technology, AhnLab MDS detects malware at the exploitation phase where vulnerable applications are exploited. Moreover, it can detect exploits that use zero-day vulnerabilities.



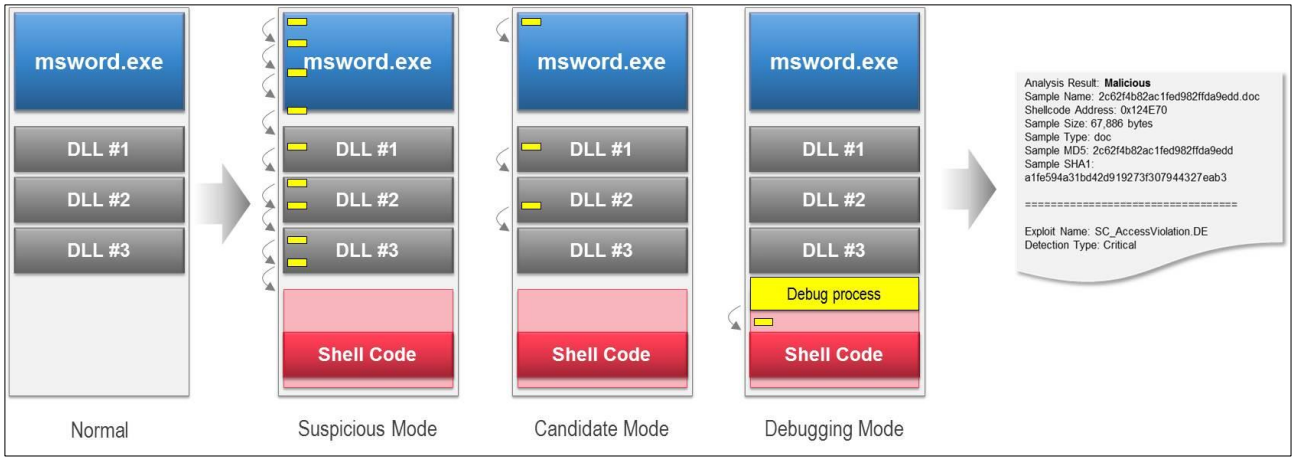
[Figure 1] Concept of Dynamic Intelligent Content Analysis

Figure 1 shows the concept of Dynamic Intelligent Content Analysis adopted by AhnLab MDS. If a malware successfully exploits a specific vulnerability of the application, there are two stages before the final behavior occurs: a pre-exploitation phase which is the stage before the malware is executed and an exploitation phase in which the malware is actually executed.

In this case, behavior-based analysis would be useless for detecting malware if it were executed properly at the pre-exploitation phase or if its malicious behavior remained hidden at the exploitation phase and thus eluded identification by a virtual machine or sandbox.

In order to prevent these sophisticated threats, it is necessary to detect malware at the pre-exploitation and exploitation phases regardless of whether behaviors occur or not. AhnLab MDS detects malware at the “pre-exploitation phase” with its Dynamic Intelligent Content Analysis technology and thereby distinguishes itself from other strategies based on a limited sandbox-based behavior analysis.

How Dynamic Intelligent Content Analysis of AhnLab MDS Works



[Figure 2] How Dynamic Intelligent Content Analysis Works

Figure 2 shows diagrams of memory structures. The table on the far left labeled “Normal” in Figure 2 is the memory structure of normal MS Word files. When a normal MS Word file is executed, “winword.exe,” the main program, and the related dynamic library files are loaded in the memory. The file is opened when all processes run properly to DLL #3.

In a case where a vulnerable MS Word file is exploited, the program runs as normal at the beginning but at some point the shellcode is saved on the heap, which is the area for saving data. Then, when buffer overflow occurs, EIP jumps to the shellcode instead of DLL#3 where the EIP was meant to move.

AhnLab MDS detects this type of malware with Dynamic Intelligent Content Analysis technology: it detects the move or jump to the abnormal memory area by inserting a debugging thread when the program is loaded in the memory. Dynamic Intelligent Contents Analysis detects the exploits at the exploitation phase, which use various vulnerabilities such as Structured Exception Handing (SEH), Return-to-Lib (RTL), Return-Oriented Programming (ROP) and heap spray as well as buffer overflow. In other words, AhnLab MDS detects malware regardless of the occurrence or types of behaviors.

Conclusion

AhnLab MDS has adopted Dynamic Intelligent Content Analysis, the exclusive technology which is implemented based on scores of algorithms developed by AhnLab's security experts. Some of the latest malware's tactics that Dynamic Intelligent Content Analysis can detect are as below:

- Vulnerability exploitation techniques such as ROP (Return-Oriented Programming) and SHE (Structured Exception Handling)
- Payload delivery techniques such as heap spray

In addition, AhnLab MDS identifies precisely the memory start point of malicious file that exploits application vulnerabilities and visualizes the shellcode memory dump and its assembly code. It is this technology that detects shellcodes by analyzing the memory and providing the precise starting address of shellcodes that distinguishes AhnLab MDS.

In terms of analysis technique, Dynamic Intelligent Content Analysis of AhnLab MDS might not be itself a brand new technology for malware analysts or security researchers. However, due to the fact that this technology has been employed in an automated analysis system (that is, AhnLab MDS) where it has been possible to analyze numerous files, it can be regarded as having opened a new era of malware analysis and of preventing APTs that use sophisticated malware.

With Dynamic Intelligent Content Analysis, AhnLab MDS detects malware without being affected by any conditions such as analysis environment or execution conditions and it provides proactive defense against the advanced targeted attacks.

AhnLab,Inc.
2310 Walsh Avenue, Santa Clara, CA 95051
www.ahnlab.com
Tel : +1.800.511.Ahnlab (1.800.511.2465)
Email : info@ahnlab.com